Project: State of Washington Multi-Agency Forest Project

Title: Forest Escalation Process

Version: 1.0

Status: Approved

Date: July, 2001

State of Washington

Windows 2000 Root Domain

Escalation Process

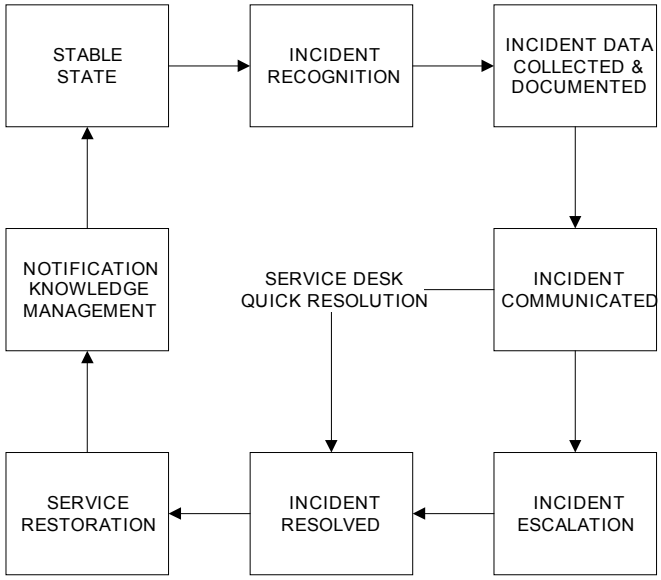
Incident and Problem Management

Document History

Status:	In development
Authors:	Anthony Witecki, Microsoft Consulting Services John Ditto, DIS
Reviewers:	Lance Calisch, DIS

Table of Contents

Incident Management Life Cycle



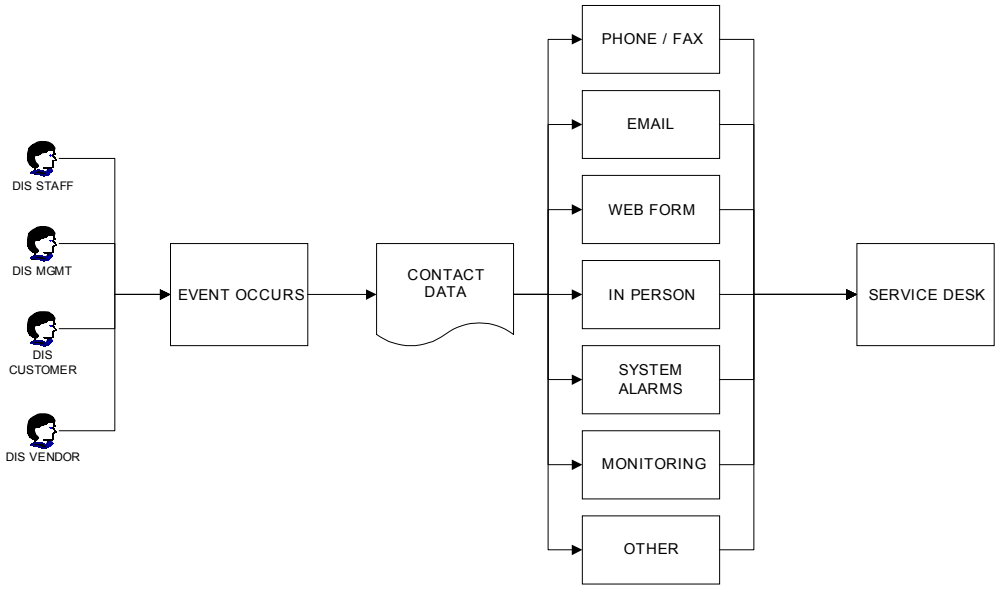
The life cycle of an incident is contained within the incident management process. In all instances, the service desk handles the initial contact. When contacted, the service desk searches the incident tracking tool for previous history on the incident and any relevant change requests that are involved.

If the service desk discovers previous history, resolution, and workarounds, it resolves the incident accordingly. If no history is found, it attempts to resolve the incident. If the service desk cannot affect resolution of the incident it is escalated to the escalation partners. The escalation partner either brings the incident to resolution, or finds a workaround if no resolution is otherwise available.

When the service desk brings an incident to resolution, it is responsible for updating the incident tracking system. Incident control ensures that incidents are reported, recorded, tracked, and resolved as quickly as possible with minimal disruption to the business processes and functions affected by the event. Incident control is the composite result of all of the activities within the incident management process.

To facilitate the incident management process, the service desk gathers information. Depending on the organization, this required information may vary between customers or customer groups. To ensure that the proper information is contained in each incident record, the service desk defines required fields in an incident tracking tool for this information. DIS uses a mainframe-based application, InfoMan, to communicate and correct events that have an adverse affect on customer service. When delivery of a DIS service is interrupted or degraded, the event is reported, assigned and resolved.

Incident / Problem Recognition



A problem is an event that interrupts or degrades the delivery of a DIS service. The event may be clearly recognized as a problem as in the case of a service interruption or only perceived as a problem in the case of slow response time caused by degraded service. These events are reported to the DIS Help Desk or the responsible service group by:

1. DIS staff
2. DIS management
3. DIS customers
4. DIS vendors

In general, a Problem Management Record should be created whenever a problem occurs. Procedures at the departmental or service group level can be used to identify events not requiring a Problem Management Record. Service Managers can identify events occurring within their area of responsibility which do not require Problem Management Records by providing procedures to identify those events.

For the Windows 2000 Root Domain, the service desk should have access to tools that enable:

1. Assess the impact of failures on customers
2. Identify customers affected by the failure
3. Establish contact processes to make all parties impacted aware of the problem
4. Retrieve, document, and track all relevant data
5. Alert (escalate) to Microsoft product support
6. Resolve issue

The service desk can effectively assess the impact of failures on and identify exactly which customers or sites are affected with an incident

tracking tool that is pre-programmed to search for and identify trends in incidents as they are reported. Typically, these tools have built-in alarms that notify the service desk when a pre-determined threshold of reports for the same type of event is received.

Incident Documentation and Data Collection

Information about a service interruption is gathered and recorded in the on-line Problem Management system for purposes of problem tracking, change control, and historical reference. The initial entry is created in the on-line database by the Problem Identifier or Problem Owner unless this person is a DIS customer who does not have access to the on-line database. In this situation, the DIS Help Desk will create the initial entry for the customer. The entry will identify:

1. The system where the event occurred
2. The severity of impact on customers
3. Customers, sites, etc. affected by the problem
4. The component causing the service interruption
5. The date and time of the interruption
6. A description of the problem
7. Parties impacted by the problem who need to be made aware of the problem.

The person creating the initial entry will identify the component causing the service interruption and assign it to the service group responsible for the failing component. The assigned service group then becomes the Problem Owner and is notified by the person making the assignment.

In situations where the nature of the service interruption prevents the immediate recording of the event in the on-line database, the information will be temporarily recorded and entered when the service is restored.

Problems are grouped into the following categories based on the identification criteria. This table is meant to be used as a guideline as a single incident may be categorized across multiple criteria.

CRITERIA	LEVEL 1	LEVEL 2	LEVEL 3
Impact on Customers	1 Customer Group	More than 1 Customer Group	All Customers
Customers, Sites Affected	1 Site	More than 1 site	All Sites
Security Weakness		Minor Threat	Major Threat
Service Outage	Single Server in Redundant Array	Service performance	Service Completely Out

Incident Communication

Event notification is the responsibility of all DIS Data Center employees and the method used for notification is based on the nature and extent of the service interruption. The DIS Help Desk is the central collection

point for this information. The procedure used in event notification is documented in Notification Management, Section 22.

Communication procedures for incidents with the Root domain will be forwarded to members of the Forest Resource Group if deemed necessary by DIS and if the extent of the problem is likely to affect the larger group.

Incident Analysis and Escalation

The Problem Owner determines if the problem can be solved within their service group or should be transferred to another service group. The Problem Owner evaluates the problem severity, priority, and complexity and invokes problem escalation procedures, as required. When the cause is determined, a plan is developed to correct it. In some situations a temporary solution can be implemented immediately while a permanent solution may take place at a later date and time. The DIS Help Desk should be updated on an hourly basis as a plan of action is developed.

Problem escalation is the process of raising the status level of a problem and awareness level to upper management and customers. Problems are evaluated in terms of the length of outage, the number of customers being impacted, the importance of the problem, and the number of times the problem has occurred.

Problems prioritized as level 2 or level 3 should be escalated to Microsoft Product Support Services immediately, unless a well-known, well-documented fix has already been made available through Microsoft.

At a minimum, the following information should be readily available to the support engineer handling the PSS Support case.

1. A clear, concise description of the reported incident
2. Error messages or issues that the customer has experienced
3. Any and all resolution techniques that the service desk has applied toward incident resolution and the results of the attempt
4. The reasons why the incident was not resolved at a given level and escalated to the next
5. The methodology and tools to use in order to properly track the escalated incident

Problem Resolution and Service Restoration

A permanent solution to the problem is developed and implemented subject to management and customer acceptance. The Problem Management Record is updated and closed by the Problem Owner after the permanent solution is successfully implemented and accepted.

Closing a Problem Management Record should take place within two working days of the problem resolution. If no agreement is reached on

resolution, the problem is thoroughly documented and the Problem Management Record is placed in suspended status but remains open.

When coming to a resolution, the service desk and its escalation partners can take one of three courses of action:

1. *Eliminate the disruption.* This indicates that the source of the incident was an isolated one. The cause of the incident was not infrastructure related, was resolved and is not expected to recur.
2. *Create a workaround for the disruption.* This indicates that the source of the incident has the potential to affect other customers. It is not expected to be isolated to a particular customer. It is related to an infrastructure CI but does not necessarily represent a significant infrastructure failure. It is, rather, a glitch in operations, a minor infrastructure event. The result is a tolerance for the incident within the organization, and a method for IT to execute a workaround to get the customer back into productive service in the event of a recurrence.
3. *Designate the disruption a known error*. This indicates that the source of the incident has the potential and is expected to recur and significantly affect other customers. It is not isolated to the particular customer. It is related to a significant infrastructure failure that requires remediation. IT is expected to execute a permanent resolution in the future through the problem management process in the long term. In the short term, there is no solution but a workaround is developed to get the customer back into productive service in the event of a recurrence.

Resource allocation ensures that appropriate resources are available and applied to the incident management process to result in resolution as quickly as possible with minimal impact to the business processes affected by the incident. The components of resource allocation are:

1. *Skill requirements.* The proper identification of the skill sets required to effect resolution is not as straightforward as it may seem. The disruption may be in one particular incident, but full resolution may require other, not-so-obvious skill sets. Accurately and thoroughly identifying all of the actual teams and relative skill requirements as early in the process as possible facilitates the incident management goal of returning the customer to productivity as quickly and efficiently as possible.
2. *Scope requirements.* The proper identification that the skill sets required by the incident are within the scope of the SLA that DIS has with its customers eliminates wasted effort for restoration of non supported services.
3. *Resource skill inventory.* The verification that the correct skill sets is possessed by DIS serves two areas. First, quick deployment of the required resources toward resolution is facilitated if the resources are internally available. If the required resources are not available, alternate resources may have to be engaged.

4. *Resource availability.* The verification that the correct skill sets are available in the correct number by each skill set provides a gap analysis that indicates the skill deficiencies and identify those skills that must be acquired to bridge the gap.
5. *Resolution within expectations.* This concerns proper and effective customer expectation management. Expectation management is cornerstone to incident management. If the customer is aware of deficiencies and is given accurate information as to actual timeframes, the customer usually understands and accepts the alternate resolution timeframe.

The service desk is responsible for Incident Closure. An incident is considered closed when the customer agrees that resolution is affected to satisfaction and all documentation and further actions designated as necessary are implemented.

Problem Reporting & Knowledge Management

The information gathered during problem tracking is stored for historical and reference purposes. This information is a valuable aid in analyzing and solving future problems and in identifying long-term solutions to reoccurring problems. Reports are available from the on-line system to support Problem Management. Contact the DIS Problem Management Administrator for more information. The DIS System Manager, DIS Disaster Recovery Coordinator, and Assistant Director will review:

1. All unscheduled system interruptions which exceed one hour.
2. Situations where multiple interruptions in a service occur in a 24 hour period.
3. When a major subsystem or an application is down for over three hours.

Information management may be automated, manual, or a combination of the two. It steps beyond individual incident record quality, and encompasses the structure and quality of the knowledge base and available documentation as a whole. When structuring incident records for ease of searching:

1. Be sure that incidents are recorded in a set format
2. Define consistent error message recording
3. Set keywords for keyword searching, if applicable
4. Eliminate conversational language and extraneous material
5. Be sure that complete solution steps are recorded